UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

NATIONAL CITY BANK, N.A., Plaintiff, v. REPUBLIC MORTGAGE HOME LOANS, LLC, JOSH WESTMARK, SUSAN TALLMAN, TAMIEKO CODUTE, and SOUN MOFFETT, Defendants.	No. C09-1550RSL ORDER DISMISSING COMPUTER FRAUD AND ABUSE ACT CLAIM AGAINST INDIVIDUAL DEFENDANTS

This matter comes before the Court on the individual defendant's "Motion to Dismiss CFAA Claim." Dkt. # 55. Defendants argue that the Computer Fraud and Abuse Act ("CFAA") claims asserted against defendants Josh Westmark, Tamieko Codute, and Soun Moffett fail to satisfy the heightened pleading requirement of Bell Atlantic Corp. v. Twombly, 550 U.S. 544 (2007), and that defendant Susan Tallman is entitled to summary judgment because plaintiff has abandoned the factual allegations against her. In the alternative, defendants argue that relief under the CFAA is unavailable even if the Court considers the facts asserted by plaintiff in its opposition.

I. ADEQUACY OF PLEADING

In the context of a motion to dismiss, the Court's review is generally limited to the contents of the complaint. Campanelli v. Bockrath, 100 F.3d 1476, 1479 (9th Cir. 1996). When determining whether a complaint states a claim upon which relief can be granted, the allegations

contained therein are accepted as true and construed in the light most favorable to plaintiff. In re Syntex Corp. Sec. Litig., 95 F.3d 922, 925-26 (9th Cir. 1996); LSO, Ltd. v. Stroh, 205 F.3d 1146, 1150 n.2 (9th Cir. 2000). The Court need not, however, accept as true legal conclusions masquerading as factual allegations, such as "defendants entered into a conspiracy to prevent competitive activity." Ashcroft v. Iqbal, ___ U.S. ___, 129 S. Ct. 1937, 1949-50 (2009). "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." Iqbal, 129 S. Ct. at 1949. Plaintiff must allege facts in support of its legal conclusions that give rise to a reasonable inference that defendant is liable for the misconduct alleged. Iqbal, 129 S. Ct. at 1949; Bell Atlantic Corp. v. Twombly, 550 U.S. 544, 556 (2007). As long as the complaint, taken as a whole, gives rise to a plausible inference of actionable conduct, the claim will not be dismissed. Twombly, 550 U.S. at 555-56.

Defendants Westmark, Codute, and Moffett challenge the adequacy of the allegations related to the CFAA claim asserted against them. Having reviewed the allegations of the Complaint for Damages and Injunctive Relief, the Court finds that they do not provide 'fair notice' of the nature of plaintiff's CFAA claim against defendants Westmark, Codute, or Moffett or the 'grounds' on which the claim rests. See Twombly, 550 U.S. at 555 n.3. No facts are alleged linking these defendants to a computer or otherwise giving rise to a reasonable inference that they could be liable under the CFAA. Iqbal, 129 S. Ct. at 1949. Plaintiff simply states the elements of a CFAA claim and alleges that defendants' conduct satisfies those elements. Complaint at ¶¶ 65-69. There are no well-pled factual allegations in support of these conclusory statements. Plaintiff's CFAA claim against Westmark, Codute, and Moffett therefore fails to state a claim to relief that is plausible on its face and is hereby DISMISSED.

II. SUMMARY JUDGMENT

In contrast to the lack of factual allegations in support of a CFAA claim against Westmark, Codute, and Moffett, plaintiff makes specific allegations against defendant Tallman

regarding unauthorized access to a National City account maintained by a third-party service provider. Complaint at ¶¶ 25 and 26.[1] Rather than contest the adequacy of these allegations, defendant Tallman argues that they are untrue, offering evidence that her new employer utilizes the same third-party service provider and that the access of which plaintiff complains was obtained using Republic Mortgage's account. Decl. of Susan Tallman (Dkt. # 16).

The declaration and exhibits submitted by defendant Tallman are not referenced extensively in plaintiff's complaint, do not form the basis of plaintiff's claim, and are not subject to judicial notice. Both parties recognize that the provision of matters outside the pleadings for the Court's consideration converts Tallman's request for dismissal into a motion for summary judgment pursuant to Fed. R. Civ. P. 12(c) and Fed. R. Civ. P. 56. Defendant can therefore prevail only if plaintiff "fails to offer evidence from which a reasonable jury could return a verdict in its favor." Triton Energy Corp. v. Square D Co., 68 F.3d 1216, 1221 (9th Cir. 1995).

Plaintiff offers no evidence in support of its allegation that Tallman improperly accessed National City's account after she resigned. A reasonable jury could not, therefore, return a verdict in plaintiff's favor on the CFAA claim as alleged. To the extent plaintiff's CFAA claim is based on Tallman's alleged use of Rapid Reporting's services, summary judgment is appropriate.

III. LEAVE TO AMEND

Without responding to defendants' challenge to the adequacy of its pleadings, plaintiff seeks to add allegations through its opposition to defendants' motion. Plaintiff accuses the individual defendants of various computer-related activities that may or may not state a CFAA claim. In order to determine whether an amendment of the operative pleading would be beneficial, the Court assumes that plaintiff's new allegations against each defendant are true and

[1] Although not clearly stated, the Court assumes that the Rapid Reporting account was computerized, potentially bringing the alleged access within the scope of the CFAA.

considers whether they state a claim upon which relief can be granted.

A. Josh Westmark

While at National City, defendant Westmark created or caused to be created an Excel spreadsheet on National City computers. The spreadsheet included confidential customer information and loan data regarding hundreds of National City customers. Westmark had access to the spreadsheet while employed by National City. Before he resigned his position, Westmark made a copy of the spreadsheet and brought it with him to Republic Mortgage in violation of National City's policies.[2] The Court will assume, for purposes of this motion, that at the time Westmark accessed and copied the spreadsheet, he was acting for the benefit of himself and/or Republic Mortgage, not his then-employer, National City.

The CFAA prohibits "accessing computers without authorization or in excess of authorization, and then taking specified forbidden actions, ranging from obtaining information to damaging a computer or computer data." LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1131 (9th Cir. 2009).[3] Plaintiff argues that because Westmark did not have permission to do

---

[2] Pursuant to a policy memorandum dated September 18, 2008, "[t]he copying and disclosure to non-affiliated persons or entities for any reason of any non-public customer personal information without their prior written consent is strictly prohibited" and "National City employees are never to download, copy or otherwise duplicate customer lists, prospective customer lists or any data containing private non-public customer information with the intent to disclose it to a third party outside National City by any means (including email) or within National City to a person without an absolute need to know the information." Decl. of Joe Cartellone, Ex. B (Dkt. # 65). An Information Security and Customer Privacy policy issued on June 12, 2009, prohibits the download of system data or customer information to portable devices and reminds employees that "all confidential information regarding past, current and potential customers is the property of the mortgage company and may not be taken with you if your employment with National City Mortgage ends." Decl. of Joe Cartellone, Ex. C (Dkt. # 65).

[3] 18 U.S.C. § 1030(a)(2) prohibits "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer." Section 1030(a)(4) subjects one who "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in

what he did, namely to download customer information and/or to retain the information after leaving National City's employ, he exceeded his authorized access in violation of the CFAA. It is important to note that plaintiff seeks to impose liability under the CFAA not because Westmark accessed the customer information improperly or without authorization, but because of what he did with the information after he accessed it. For the following reasons, the Court finds that the CFAA was not intended to, nor should it, stretch so far.

First, when determining whether a CFAA violation has occurred, the statutory language suggests that the key issue is whether the defendant had a right to access the computer or computerized information (*i.e.*, whether the access was "authorized"), not whether he or she misused the information thereafter. One has authorization to do something if permission or power to do so is granted by a recognized authority. See LVRC Holding, 581 F.3d at 1133. Under the CFAA, the activity that must be authorized is the "access," not the use to which the information is later put. When an employer grants an employee access to a computer system or to certain records on a computer system, access continues to be authorized until rescinded by the employer, even if the employee has become disloyal and is acting contrary to the employer's interest. LVRC Holdings, 581 F.3d at 1133-34 (discussing Int'l Airport Ctrs. LLC v. Citrin, 440 F.3d 418 (9th Cir. 2006)). Whether access to a computer is "authorized" is determined by the scope of the permission granted by the employer, not by the employee's state of mind.

The phrase "exceeds authorized access," which is defined in the statute, means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). The Ninth Circuit has distinguished "without authorization" and "exceeds authorized access" as follows:

---

any 1-year period" to liability. A "protected computer" includes any computer used in or affecting interstate commerce. 18 U.S.C. § 1030(e)(2)(B).

> [A] person who "intentionally accesses a computer without authorization" . . . accesses a computer without any permission at all, while a person who "exceeds authorized access" . . . has permission to access the computer, but accesses information on the computer that the person is not entitled to access.

LVRC Holdings, 581 F.3d at 1133 (statutory citations omitted).[4] A CFAA violation occurs only when an employee accesses information that was not within the scope of his or her authorization. The CFAA was not intended, and should not be read, to criminalize wrongs that fortuitously involve the use of a computer: otherwise, any misuse of corporate information (such as embezzlement or insider trading) would give rise to a CFAA violation merely because the information was at some point stored in a computer system. See US Bioservices Corp. v. Lugo, 595 F. Supp.2d 1189, 1193-94 (D. Kan. 2009) (noting that Congress was targeting crimes that had at their core the use of a computer and was not interested in frauds that could have occurred just as easily had the information been obtained from a wastepaper basket).

It is undisputed that Westmark was authorized to access, view, and utilize the Excel spreadsheet that forms the heart of plaintiff's CFAA claim against him. There is no indication that Westmark accessed or obtained any information from National City's computers after he resigned his position with National City. If, as is the case here, the employee were entitled to access the materials at issue, nothing in the CFAA suggests that the authorization can be lost or exceeded through post-access conduct. See LVRC Holdings, 581 F.3d at 1135 n.7; US Bioservices, 595 F. Supp.2d at 1195. On the other hand, if an employee's access is limited to certain documents, files, or drives, an effort on his part to delve into computer records to which he is not entitled could result in liability under the CFAA. This interpretation gives effect to the language of the statute, furthers its purpose of combating the unauthorized procurement or

[4] Whether the absence of relevant employer policies was material to the Ninth Circuit's decision in LVRC Holding is doubtful: the court makes note of the lack of policies in the fact section, but does not rely upon it in the CFAA analysis.

alteration of information, and is consistent with the legislative history.

Second, the CFAA is predominantly a criminal statute, the interpretation of which should be neither surprising nor novel. LVRC Holdings, 581 F.3d at 1134. The statute "was enacted in 1984 to enhance the government's ability to prosecute computer crimes. The act was originally designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality . . . ." LVRC Holdings, 581 F.3d at 1130. An employee who has permission to access a range of documents and stays within the confines of his authorization would have no reason to suspect that he could be charged with hacking, *i.e.*, exceeding his authorized access, simply because he uses those documents in a way that violates company policies regarding confidentiality or document retention.

Finally, there is no reason to believe that Congress intended to create a federal enforcement mechanism for corporate policies regarding document handling and retention when it enacted the CFAA. Employers already have a number of tools with which to enforce confidentiality, non-competition, and document retention policies. They can discipline erring employees, file a breach of contract or breach of fiduciary duty claim, sue for conversion, and/or seek injunctive relief. Neither the purpose of the CFAA nor its language suggests that the misuse of computerized information that was legitimately accessed by the employee triggers civil or criminal liability.

Plaintiff cites a number of cases for the proposition that an employee exceeds his authority to access information when he acts in a manner than is inconsistent with company policies. See, e.g., EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581-84 (1st Cir. 2001). While there is a clear split in authority on this point, the Court finds persuasive those decisions which consider the purpose of the CFAA and the distinction between unauthorized access and unauthorized use of legitimately-accessed materials.

The Court therefore concludes that, in order to state a cause of action under 18

U.S.C. § 1030(a)(2) or (a)(4), plaintiff must allege that Westmark either accessed its computer system without authorization or exceeded his authorized access by accessing documents, files, or drives to which his authorization did not extend. Plaintiff makes no such allegation. Instead, its CFAA claim relies solely on the allegation that Westmark misused the documents that were on his computer in violation of company policies. Because plaintiff's revised and supplemented allegations do not establish a cause of action under the CFAA, amendment would be futile.

B. Tamieko Codute

Defendant Codute is accused of attempting to lure National City customers to Republic Mortgage by sending personalized letters that imply a certain level of knowledge regarding the customer's current interest rate and loan term. Plaintiff hypothesizes that "Codute likely retained a customer list, electronically or otherwise, that she has been using to solicit National City customers." Opposition at 8. Even if this assumption were true, it does not appear that plaintiff can, consistent with its Rule 11 obligations, allege a violation of the CFAA. Plaintiff is unable to state that Codute obtained the customer list from a protected computer or that her access to the computer and/or the customer list was unauthorized. The crux of plaintiff's claim against Codute appears to be that she has retained confidential customer information after she left National City's employ in violation of National City's policies. Even if the alleged breach of policy involved the use of a computer, it would not trigger liability under the CFAA for the reasons stated above.

C. Soun Moffett

It is not clear how defendant Moffett is supposed to have violated the CFAA. There is no indication that Moffett ever worked for National City or accessed any of its computers or computerized information. At most, Moffett saw National City's customer information when the other defendants brought it to Republic Mortgage. Plaintiff cannot assert a CFAA claim based on this happenstance.

D. Susan Tallman

Having abandoned the only allegation of computer access actually found in the complaint, plaintiff accuses defendant Tallman of supervising employees who may have violated the CFAA. At her deposition, Tallman was asked whether any of the loan officers at National City had kept customer lists or information after they left National City's employ. Tallman indicated that she assumed they had done so "[b]ecause it's their job." Tallman Dep. at 66. Plaintiff argues that Tallman should be held vicariously liable for the CFAA violations of her subordinates.

Whether a supervisor can be vicariously liable under the CFAA is an open question. Although vicarious liability is the norm in tort law, the CFAA is primarily a criminal statute designed to punish intentional frauds. The case upon which plaintiff relies as support for its broad theory of vicarious liability involved a situation where the defendant affirmatively urged its recruit to access a computer system beyond his authorization. Charles Schwab & Co., Inc. v. Carter, 2005 WL 2369815 at *7 (N. D. Ill. Sept., 27, 2005). Even if Carter controls, there is no allegation that Tallman engaged in any culpable behavior or caused her subordinates to violate the CFAA. Even if plaintiff could assert that Tallman urged her subordinates to download and retain National City's computerized information, because her subordinates had authority to access the information at issue, plaintiff would not be entitled to relief under the CFAA.

IV. CONCLUSION

For all of the foregoing reasons, defendant Westmark, Codute, and Moffett's motion to dismiss is GRANTED. Defendant Tallman's alternative request for summary judgment is GRANTED. Because plaintiff has no evidence (or even suspicions) that would support a CFAA claim, the claim is DISMISSED with prejudice and without leave to amend.

DATED this 12th day of March, 2010.

Robert S. Lasnik
United States District Judge